COSMOS
Navigate the Compliance Universe

Compliance Risk Assessments - An Introduction
Chapter 4. Step Two: Determining Likelihood of Occurrence

Chapter Goals:

- Develop compliance risk factors that are specific to your business, industry, and country.
- Understand how to prioritize the compliance risk factors, which includes assessing the likelihood of the risk's occurrence.

Two compliance risk factors are typically used to determine the risk level of a compliance issue—*likelihood of occurrence* and *impact of occurrence*. It is with these two factors that you will be able to turn your risk universe list into a risk universe matrix—a graphical representation of risks that can help prioritize your risk mitigation efforts.

General Overview

In general, *likelihood of occurrence* is the probability that noncompliance with a law or regulation will occur daily, monthly, yearly, once every five years, ten years, etc. *Impact of occurrence* is the degree to which a noncompliant incident will have a negative effect on the business in terms of financial resources being depleted, your CEO going to jail, damage to the corporate reputation in the eyes of the public, or even a more practical issue—a data breach resulting in disclosure of personally identifiable information (PII).

It is both the likelihood and the impact of occurrence that will help your compliance team determine how the business will prioritize the compliance risks. If the likelihood of an occurrence of noncompliance is every five years and the impact on the firm is minimal (say, a fine of $1,000), this risk would be relatively low in terms of concern to the business. Of course, this does *not* mean that you should ignore this risk. Rather, this scenario of an unlikely incident coupled with a low impact caused by the incident means that this noncompliance issue is probably one you will deal with later.

In contrast, noncompliance with the law regarding payment of overtime to your employees every week for a period of years, which in the United States is a violation of the Fair Labor Standards Act, could have a devastating impact. Your business would face substantial punitive fines as well as a requirement to pay lost wages and attorney fees. It also could make a lot of employees angry, cause a tremendous amount of bad publicity, and a possible Department of Labor or Internal Revenue Service audit. Since this scenario could become a daily (or at least weekly) occurrence and have significant short-term and long-term impact, it should be prioritized to fix.

Likelihood of Occurrence

What is the probability that your business will violate a specific law or regulation? Of course, you hope the answer is "never."

More likely the answer to this question is "unfortunately, probably a lot more than I imagined." And while it is

desirable that the noncompliance is an unintentional act with no malice intended, measuring the likelihood of noncompliance also incorporates the possibility of an intentional act.

Likelihood of occurrence uses two factors—*controls* and *frequency*—to determine the potential for encountering it.

Figure 1 shows a sample method to evaluate the likelihood-of-occurrence factors for any form of business. This sample is generic; each business must develop a customized version based on its unique set of risks and compliance concerns in its universe.

Figure 1: Likelihood of Occurrence Factors

Likelihood of Occurrence Factors			
Rank/Scale		**Measure of Likelihood**	
		Existing Controls	**Frequency of Noncompliance**
1	Rare	• Policies mandated and updated regularly • Regular mandatory training is provided to the identified responsible person(s)* and is documented • Regular management monitoring reviews are performed and documented	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	• Policies mandated and updated regularly • Regular training is provided to the identified responsible person(s), but not documented * • Regular management monitoring reviews are performed, but not documented	Could occur at some time At least once in 10 years
3	Possible	• Policies mandated, but not updated regularly • Responsible person(s) identified* • Training is provided when needed • Some management monitoring reviews are performed, but not documented	Might occur at some time At least once in 5 years
4	Likely	• Policies and procedures in place but neither mandated nor updated regularly • Responsible person(s) identified* • Some formal and informal (on-the-job) training • No management monitoring reviews	Will probably occur At least once per year

5	Almost Certain	• No controls in place • No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews*	Expected to occur in most circumstances More than once per year

*Identified responsible person(s). This term refers to any individual(s) in your organization who is responsible for ensuring that he/she knows that there is a law and is empowered by your organization to bring the entity into compliance with the law and to monitor continued compliance the law. Sometimes this person is called a Compliance Partner or other similar terminology to reflect the importance of the employee within this compliance structure.

Existing Controls

Existing controls shape behavior. Controls could be policies, procedures, training, or any method of controlling behavior that is effective at your business. Perhaps your firm has a particularly strong culture of compliance so that noncompliant behavior is simply not expected and is clearly not condoned. Perhaps you have a systematic (and documented) training program that highlights key areas of noncompliance and how to report any concerns about noncompliance. Whatever your controls, they are existing controls—controls in place at your business designed to ensure that it is complying with a law or regulation.

The fewer controls in place, the more likely that an issue of noncompliance will occur. The fewer controls that are known to employees, the more likely an issue of noncompliance will occur. Employees need to know what they are responsible for doing (and not doing) and need to be aware of the consequences for noncompliant actions. Taking a very dim view of society, it is possible that when the business does not have controls in place and has not informed employees of these controls, employees may likely make wrong choices. That is not a culture to be proud of; it is a reality where taking the wrong action might take less time and energy than taking the right action. And this could be the case if the employer does not have the right controls in place to stop this action.

Your compliance team should use the factor of existing controls to help determine the level of compliance risk.[1]

Rank/Scale

The first column in Figure 1 is titled "Rank/Scale" and ranges from 1 to 5. Number 1 represents a simple numeric indication of the *lowest* likelihood of the risk occurring while 5 represents the *highest* likelihood of the risk occurring.

In the adjacent column, a descriptive term for each numeric rank is provided. These range from "Rare" to "Almost Certain." "Rare" represents the lowest likelihood of the risk occurring, while "Almost Certain" represents the highest likelihood of the risk occurring.

The numbers and the terms represent the exact same thing, but it is sometimes helpful for readers of factor matrixes to see words as well as a numbering system to describe a category.

Existing Controls

Using the five-step rating system, if you or the compliance committee were to evaluate a law and determine that

the likelihood of noncompliance with this law was a "1" or "Rare," that could mean that your business has existing controls and policies in place that are effective. Regularly scheduled and mandatory training is provided to the person/people responsible for ensuring compliance with the law within your organization. Their training is documented and regular monitoring by management is performed and documented.

Similarly, if your compliance team evaluates a law and indicates that the likelihood of a noncompliance is a "5," or "Almost Certain," your business clearly has ineffective or none of the following: controls, policies or procedures, person responsible for monitoring compliance, awareness training, or monitoring by management put in place.

Likewise, 2 through 4 rankings are variations of this likelihood of occurrence.

Frequency of Noncompliance

Frequency is the rate at which a compliance risk occurs. Is it likely that this compliance risk will occur once every 10 years, once a month, or once a day? It is this determination of how often a risk might occur that determines "Frequency of Noncompliance."

Using the same five-step ranking and analysis discussed above with "existing controls," if the compliance team evaluates a law and determines that noncompliance with that law is probably only going to occur in exceptional circumstances, perhaps less than once every 10 years, then the numerical value chosen for this factor would be "1." For example, if a law requires reporting to an agency once every 10 years, then this law would receive a "1" rating in frequency. In contrast, if the compliance team evaluates a law and determines that instances of noncompliance are probable in most circumstances and typically could occur more than once per year, then the numerical value chosen for this factor would be "5."

Note that this frequency column presumes quite a range of time. Customization of these factors is critical. It may be that in your industry the frequency factor should be changed to daily, weekly, monthly, yearly, and less than once a year. Adopting the definitions and frequency ranges should not occur without significant input from your colleagues responsible for implementing this overall compliance risk assessment.